安全で利便性の高い公衆無線LANを提供する次世代ホットスポット基盤Cityroam

[解 説]

安全で利便性の高い公衆無線 LAN を提供する 次世代ホットスポット基盤 Cityroam

後藤英昭
東北大学サイバーサイエンスセンター クラウドサービス基盤研究室

1　はじめに

公衆無線 LAN には，事前契約が必要な商用サービスや，携帯電話会社が提供するいわゆる「キャリア Wi-Fi」，観光客や店舗利用者がその場で利用開始できるフリー (無償)Wi-Fi などがある．現行のフリー Wi-Fi のほとんどが，暗号化のないオープン Wi-Fi によるもので，盗聴による情報窃取が容易である．端末を偽基地局に誘導することも容易であり，データの盗聴や改ざん，マルウェアの挿入，基地局からの能動的な攻撃など，セキュリティ上の重大な欠陥が多い．利用者認証のあるサービスでは，無線 LAN の接続ごとにログインの手間がかかる，不正なログイン自動化ツールによるサービス悪用，偽のキャプティブポータルによるアカウント奪取などの問題がある．また，利用するサービスごとに登録が必要で，利便性が低い．

キャリア Wi-Fi の中には，IEEE 802.1X [1] に基づいた安全かつ自動接続可能な認証方式 (通称，1X 認証) を採用したものがあり，上記の問題の多くが解決される．しかし，事前に現地の電話契約が必要という敷居の高さがあり，外国での利用は難しい．

以上のような問題を解決し，安全で利便性の高い公衆無線 LAN を実現しようとする，「次世代ホットスポット (NGH, Next Generation Hotspot)」という規格がある [2]．NGH は，Wireless Broadband Alliance (WBA) と Wi-Fi Alliance が共同で推進しているもので，1X 認証を含む Passpoint (Hotspot 2.0) を基本としており，ローミング機能も含まれる．Passpoint は，元々はキャリア Wi-Fi の高度化の色が濃いが，2014 年頃よりフリー Wi-Fi への適用も模索されている．

本稿では，国内の NGH 基盤の概要を説明する．著者らは，フリー Wi-Fi 向けの認証連携の実証実験を 2017 年より行っており，City Wi-Fi Roaming トライアルに参加することで，国際的なローミングを実現した．2018 年 6 月より，国内の認証連携基盤に Cityroam の名称を与え，通信事業者及び一般利用者に利用開放し，開発と実証実験を進めている．技術面の詳細については [2, 3] に譲り，本稿ではシステム開発の背景とサービス仕様について述べる．

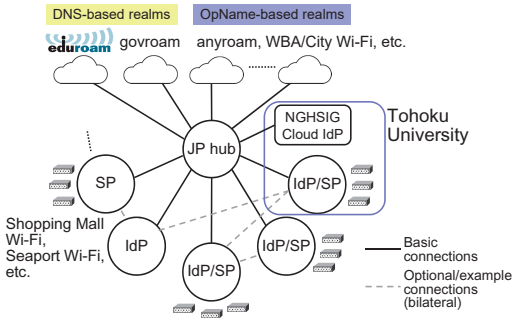

図 1　JP hub と NGH テストベッド

2　NGH テストベッドと Cityroam

2.1　開発経緯とシステム構成

日本国内では，2016 年時点で，携帯電話や公衆無線 LAN の大手事業者に NGH を推進する動きが見られなかった．また，フリー Wi-Fi のセキュリティ問題が指摘されているにも関わらず，セキュアな接続手段の導入が進んでいなかった．このような状況の下，国内の公衆無線 LAN のセキュア化と NGH 導入を推進する目的で，著者が発起人・幹事となって，2017 年 1 月に「セキュア公衆無線 LAN ローミング研究会 (NGHSIG)」を発足させた [4]．現在，当研究会が中心となって，複数の通信事業者と協働で，国内の NGH 基盤及び次世代フリー Wi-Fi の整備を進めている．

図 1 に，国内の認証連携基盤である NGH テストベッドの構成を示す．中央の JP hub に，参加機関の基地局と認証サーバが収容される．機関は，利用者のアカウントを提供して実際の認証処理を行う IdP (Identity Provider) と，基地局を設置してネットワークアクセスを提供する SP (Service Provider)，及び，両方を行うものに大別される．このテストベッドに接続された機関は，他のすべての機関と信頼関係を結んでいるとみなす．すなわち，利用者の端末がどの SP の基地局に接続を試みても，認証要求が当該利用者のアカウントのある IdP まで届けられ，認証に成功すればネットワークアクセスが許可される．

国ごとに中心となるハブを置くネットワーク構成は，元々は，複数のローミングコンソーシアム (RC,

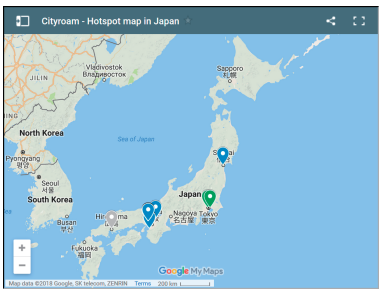

図 2　Cityroam 基地局マップ (2018 年 7 月現在)

Roaming Consortium) を相互接続するための認証連携アーキテクチャの開発の過程で考案されたものである [2]．学術系無線 LAN ローミング基盤 eduroam [5] や，これをベースに開発された政府機関向けの govroam [6] は，それぞれが一つの RC に相当する．eduroam と govroam の両方のサービスを提供しようとする SP は，SSID ごとに認証連携ネットワークを分離する必要がある．それぞれの RC には多数の機関が存在するが，それらを区別するレルムは，ドメインネームシステム (DNS) のドメイン名に基づいていることから，一般には RC を識別できるような文字列が含まれていない．Passpoint では SSID が区別できないため，認証連携ネットワークを分離できず，レルムを見ただけではどちらの RC に認証要求を転送すべきか判断できないという問題が生じる．世界中のレルムと RC の対応表を各 SP が持つのは現実的ではないが，地域ごとに RADIUS proxy を設置し，それぞれが地域内のレルムの振り分けを行うようにすれば，管理上も現実的な規模になると考えられる．

我々は，2017 年 4 月に NGH テストベッドの運用を開始して，研究会に参加している通信事業者や開発者の協力を得て，国内各地の基地局を利用した実証実験を行ってきた．国内でセキュア公衆無線 LAN サービスの展開を本格化させ，また，国内外の通信事業者・都市などとローミング契約の交渉を進めるにあたり，利用者にも分かりやすい名称が必要になったことから，国内の認証連携基盤及びサービスのブランド名として，2018 年 6 月より Cityroam™ の名称で呼ぶことにした．図 2 は執筆時点の基地局マップである．

2.2　Cityroam のサービスと仕様

Cityroam は，公衆無線 LAN の中でも主にフリー Wi-Fi を対象としており，現時点では国内のみの基盤である．フリー Wi-Fi の収益構造が一般に局所的に閉じていることを利用し，従来の商用無線 LAN サービスのローミングと異なり，通信事業者間でローミング使用料の授受を仲介するような機能は提供しない．これにより支払いシステムの煩雑性を排除し，通信事業者や都市などが気軽に利用できる，軽量の認証連携基盤を目指している．ただし，基盤自身の運用のために，システム使用料は必要である．IdP の事業者と SP の事業者の間で，Cityroam を仲介しない形でローミング使用料の授受を行うことは，妨げない予定である．

学術系無線 LAN ローミング基盤 eduroam を知っている人なら，教育研究機関の構成員に限らず「一般市民が利用できる eduroam 風のサービス」と考えれば，Cityroam のサービス内容をほぼ的確に理解できると思われる．実際のところ，Cityroam の技術的な仕様や運用方式は，eduroam を手本にしたものである．Cityroam では SP と IdP が別々の事業者のことが多いため，認証連携に参加することで各事業者が得られるメリットという観点が重要であり，この部分が eduroam にある「互恵精神」とは異なる．

2.3　サービスプロバイダ (SP) の仕様

Cityroam では，NGH の国内展開を目標としていることから，SP では Passpoint の対応を基本としている．しかしながら，使用中の基地局が Passpoint に非対応ですぐに更新できなかったり，対応品でもまだ互換性に難のある製品があるため，現時点では Passpoint 対応を要件とはしていない．すなわち，1X 認証のみのサービス提供も可能である．

Cityroam では，1X 認証や Passpoint を用いたセキュア接続を必須としている．そのため，eduroam の規程と同様に，キャプティブポータルを利用したいわゆるウェブログインの提供は禁止されている．Cityroam では共通の SSID として “cityroam” を使用する．これにより，Passpoint に非対応の端末も，一度設定を行うだけで全国の基地局が利用可能となる．

Cityroam の特徴の一つに，eduroam や，政府機関向けの govroam との連携が挙げられる．Cityroam では，これらのサービスを併設することを標準としている．これは，eduroam/govroam の市街地サービスの充実を目指したものであり，世界的にもニーズの高いこのようなサービスを容易かつ低コストで実現する枠組みを開発・提案することで，両方のコミュニティにも貢献が期待される．eduroam/govroam の Passpoint/NGH 対応は，eduroam の国際運用の中心機関である GÉANT と WBA の間で交わされた MoU (Memorandum of Understanding) を利用して，現在著者らが開発中であり，まだ一般に利用できる段階ではない．そのため，Cityroam の基地局では eduroam

の標準の SSID である “eduroam” も併設している．これにより，世界中の eduroam 利用者が，市街地で容易にサービスを享受できるようになっている．govroam については，2018 年 7 月時点で日本は未加入であり，現在サービスを提供していない．

Cityroam の SP となれるのは，通信事業者や，それに準じて eduroam を提供する教育研究機関などに限定される．公衆無線 LAN を安心して利用できるようにするために，契約の下，各 SP は盗聴や改ざんなどを行わないように義務付けられる．1X 認証では，端末が事前に正しく設定されている限り，認証連携基盤に接続していない偽の基地局では認証が失敗するため，不正なネットワークに誘導されることはない．

2.4　アカウントの仕様と IdP

アカウントに関するポリシーは以下のとおりである．

1. 一つのアカウントで，基本的にすべての参加 SP においてサービスが受けられる．
2. 個人または小規模なグループと紐付けられた，信頼できるアカウント (trusted account) を使用．
3. 不正利用が発覚した場合，IdP は該当するアカウントをすみやかに利用停止する．

ローミング環境なので，1 は自明である．すべての参加 IdP のアカウントについて，すべての参加 SP がサービスを提供することを原則とするが，ビジネスが競合するなどの特別の理由がある場合，特定の IdP と SP の間で連携を制限することも認める．

2 の「信頼できるアカウント」は，ローミング環境を実現する上で重要である．一つの事業者が IdP と SP を兼ねる場合は，アカウント発行についての責任も自前で負うことになる．一方，ローミング環境では IdP が発行したアカウントの詳細を SP が知ることはない．すなわち，SP は IdP との信頼関係を元に，アカウントを受け入れることになる．IdP は，多くの SP に信頼してもらえるような基準でアカウントを発行する必要がある．また，3 のように，インシデントなどの際に IdP は迅速に対応し，SP に対して誠実に振る舞うことが求められる．

Cityroam では，無線 LAN サービスの不正利用の対策として，個人に紐付いたアカウントの利用を前提としている．フリー Wi-Fi の中には，利用者登録が不要で，誰でも匿名で利用できるサービスが多数ある．しかし，このようなサービスは，無線 LAN サービスを踏み台として不正アクセスや大規模なサイバー攻撃を行うといった不正利用の温床になりうる．また，通信内容の個人ごとの暗号化が難しいことも問題である．アカウントを個人に紐付け，ログインを必須にすることは，不正利用の抑止力となることが期待される．万一の不正利用の際に，利用者の追跡が可能になることが，責任所在の明確化という観点で重要である．

観光客向けのフリー Wi-Fi の提供の話になると，「海外では登録不要で自由に使えるのが普通」といった言説を目にすることがあるが，これは誤った認識と言える．例えば，タイやシンガポールでは本人確認の要請が厳しく，公衆無線 LAN の利用登録にパスポートの提示が求められたりする．欧州各地の空港では，携帯電話の SMS (Short Message Service) で確認コードを受信する仕組みの利用登録がよく見られる．このいわゆる SMS 方式は，電話回線/SIM の契約時に本人確認が行われていることを利用した，間接的な本人紐付けに相当する．無線 LAN サービスの提供者と電話会社の間には何の契約もないため，仮に重大なインシデントがあり，捜査が必要となった場合でも，電話会社が協力する保証はない．従って，十分な紐付けとは言えないが，利用者の足跡をある程度記録しておける簡便な方法のため，オンラインサインアップでは広く利用されている．

本人紐付けをどこまで確実に行うかについては，法制面の整備も含めて，まだ国際的に議論が必要な段階である．現行の Cityroam では，オンラインサインアップの利便性に配慮して，SMS を最低限の本人紐付け手段とみなし，認めている．ただし，本人確認なしに SMS を提供する事業者もあることから，そのような所の SIM ではサインアップできないようにするなどの対策が必要になる．

フリー Wi-Fi で利用者登録を必須とした場合，行く先々の異なるシステムごとに利用者登録を行うのは不便なことから，ローミングによるアカウント共用が望ましい．Cityroam は，一つのアカウントで事業者間で横断利用できるシステムの構築を目指している．本人紐付けが必要な場合，無人ではオンサイト (その場) での本人確認が難しい問題がある．そのため，Cityroam では，オンサイト登録が必要な局面を極力減らすために，利用者がいずれかのサービスで登録済みのアカウントを積極的に利用するシステムの実現を目指している．例えば，インターネットサービスプロバイダ (ISP) や携帯電話などの利用者登録で取得したアカウントをはじめ，本人紐付けのある様々なオンラインサービスのアカウントも対象になりうる．ア

カウントの形式としては，ID・パスワードやクライアント証明書 (電子証明書) に加えて，携帯電話の SIM の利用も有力である．1X 認証では，SIM を利用した認証方式として EAP-SIM や EAP-AKA/AKA' を利用することができ，既にキャリア Wi-Fi などで実用化されている．

2.5 Cityroam で利用できるアカウント

2018 年 7 月時点で，以下のような IdP またはシステムのアカウントが利用可能となっている．

- 参加事業者の IdP
- NGHSIG クラウド IdP
- eduroam
- ANYROAM
- Odyssys Hotspot 2.0 OSU (デモ専用)
- City Wi-Fi Roaming (国内外の通信事業者と都市が参加, 期間中のみ有効)

NGHSIG クラウド IdP は，eduroam の代理認証システム [7] と同等の集中型認証システムであり，セキュア公衆無線 LAN ローミング研究会の参加機関が利用できる．アカウント発行の実務を担当する機関は，管理者のサインアップのみでこの IdP をウェブ上のインタフェースから操作でき，アカウントのバルク発行・ダウンロードが可能である．

ANYROAM は eduroam のインフラを利用したサービスで，教育研究機関以外の利用者も受け入れると宣言した大学などで利用可能である [8]．米国で運用されているが, 参加機関はまだ少数である．ANYROAM は SMS 方式を採用しており，オンラインで誰でも無償 (執筆時) でアカウントを取得可能である．

Odyssys Hotspot 2.0 OSU は，Global Reach Technology が無償で提供しているオンラインサインアップシステムで，様々な OS に対応した Passpoint プロファイルを取得できる．このシステムは，本人紐付けの機能がないため，Passpoint 対応システムの開発やデモに用いられる．

City Wi-Fi Roaming は，WBA が主催し，世界各地の都市で提供される公衆無線 LAN を NGH 基盤で結ぶことにより，一つのアカウントで相互利用 (ローミング) できる環境を構築しようとする，世界規模のトライアル (プロジェクト) である．第 2 回目となる 2017 年は，6 月 20 日の World Wi-Fi Day を起点として，8 月末までの期間，20 程度の都市を結んで開催された．研究会では国内の機関として初めてこのトライアルに参加し，実証実験を行った ([3] で既報)．

City Wi-Fi Roaming では，電話会社が提供する SIM 認証が利用できる．将来，この仕組みが定常的に利用できるようになれば，現地での利用登録が不要となり，自分が常用している携帯電話の SIM を用いて，フリー Wi-Fi を容易かつ安全に利用できることになる．これは，都市にとって観光客への大きなアピールになると期待されている．

3 むすび

安全で利便性の高い公衆無線 LAN を実現するために開発・展開を進めている，次世代ホットスポット基盤 Cityroam の概要を述べた．現在，Cityroam は国内のみの基盤であるが，その技術と運用方法を海外にも提案することで，世界規模の次世代ホットスポットの構築にも貢献することを目指している．Cityroam の特徴の一つとして，小規模な通信事業者でも容易に参加できることが挙げられる．一つのアカウントで利用できる範囲が広がるため，従来は利用者認証が難しかった小規模なサイトでも，安全な無線 LAN が提供しやすくなると考えられる．また，eduroam サービスの市街地展開によって，世界でも先進的な教育研究環境の実現に貢献している．

利用できるアカウントの拡充のために，国内外の通信事業者との交渉を進めている．SP となる通信事業者も随時募集している．現在，オンサイト登録を実現するシステムの開発などが課題となっている．

参考文献

[1] IEEE Std 802.1X-2010, "Port-Based Network Access Control."
[2] 後藤英昭, "次世代ホットスポット (NGH) の世界動向と NGH 対応 eduroam システムの開発," 信学技報 IA2017–61/IN2017–60, pp.49–54, 2017.
[3] 後藤英昭, 中村素典, 曽根秀昭, "デジタル時代の教育・研究を支える基盤としての eduroam と次世代ホットスポット," 大学 ICT 推進協議会 2017 年度年次大会 論文集 TC2–5, 2017.
[4] セキュア公衆無線 LAN ローミング研究会 (NGHSIG), https://nghsig.jp/
[5] eduroam JP, https://www.eduroam.jp/
[6] govroam, https://govroam.nl/english/
[7] 後藤英昭, 新妻 共, 大和純一, "大規模学術系無線 LAN ローミングのための集中型認証システム," 信学論 D, J100-D, No.5, pp.584–594, 2017.
[8] ANYROAM, https://www.anyroam.net/